SUB BI

CLAIMS

1. A method of managing a secure (7) terminal (1) used for transactions with smart cards having the following steps:

- a smart (22) card (5) is placed in contact with the terminal,

- the terminal is made to execute a program (26), this program including sensitive operations (29) related to making the transactions secure,

characterised in that

- the number of times a request is made to the terminal to execute sensitive operations is counted (32, 16), and

- the action of this terminal is restricted as soon as this count reaches (33) a fixed value.

2. A method according to Claim 1, characterised in that

- the terminal is provided with a removable electronic security circuit (8), and

- the number of requests for sensitive operations which are made to it or sensitive operations executed by it are counted (16) in this circuit.

3. A method according to either of Claims 1 or 2, characterised in that

- the sensitive operations are divided into a number of classes and

- a count (16, 17) is set up for each class.

4. A method according to one of Claims 1 to 3, characterised in that,

- as a sensitive operation, a mutual identification procedure between the terminal and the card is executed.

5. A method according to one of Claims 1 to 4, characterised in that,

- as a sensitive operation, an authentication (PIN) of a carrier of the smart card is performed.

6. A method according to one of Claims 1 to 5, characterised in that,

- as a sensitive operation, a verification of a certificate coming from a smart card is performed.

7. A method according to one of Claims 1 to 6, characterised in that

- the counter is re-initialized by a secure procedure including a verification of a secret code by the terminal or the security circuit.

8. A method according to Claim 7, characterised in that

- the secure procedure includes a verification of a secret code by the terminal or the security circuit.

9. A method according to Claim 7, characterised in that

- the re-initialization is performed remotely by a master system.

10. A method according to one of Claims 1 to 9, characterised in that

- the counter is incremented after a successful sensitive operation.

11. A method according to one of Claims 1 to 10, characterised in that

- for restricting, only some (47) of the operations of the planned transaction are prevented.

12. A security circuit for implementing the method according to any one of Claims 1 to 11, characterised in that it has management means (16, 17, 32, 39) capable of:

- identifying and counting requests coming from outside and restricting its functions as soon as the count reaches a predetermined number.